

AMENDMENTS TO THE CLAIMS

1. (currently amended) A method of updating an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:

physically separating from said wireless station a network communication device containing [[an]] said encryption key [[used in]] which is accessed for use by said wireless station during said encrypted communications [[from said wireless station]];

physically connecting said removed network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device;

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; and

physically reconnecting said network communications device containing said new encryption key with said wireless station of said network.

2. (Original) A method as in claim 1, wherein said new encryption key is generated at user-defined intervals.

3. (Original) A method as in claim 1, wherein said new encryption key is generated on user-specified days.

4. (previously presented) A method as in claim 1, wherein:

said key generator generates a first new encryption key;

compares said new encryption key to the previous k encryption keys used in said network; and

generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

5. (Previously Presented) A method as in claim 4, wherein k is a user-defined number of previously used encryption keys.

6. (previously presented) A method as in claim 1, wherein said network communication device is configured on a plug-in card and is physically connected to said network by inserting said network communications device into a card tray at said updating device.

7. (Original) A method as in claim 6, wherein a plurality of network communications devices can be inserted into said card tray simultaneously.

8. (currently amended) A wireless network comprising:

a wired station connected to a wired network, said wired station comprising:

an encryption key generator for generating an encryption key;

a network communications device for transmitting said encryption key over said wired network; and

a wired encryption key updating device connected to said wired network;

a wireless station wirelessly connected to said network and communicating with said wired network through communications encrypted with an encryption key, said wireless station comprising:

a wireless network communications device containing [[an]] said encryption key accessed by said wireless station for use in said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to an updating device wired to said network to receive and

store as a new encryption key, an encryption key transmitted over said wired network by said wired network communications device.

9. (previously presented) A wireless network as in claim 8, wherein said new encryption key is a randomly generated encryption key.

10. (original) A wireless network as in claim 8, wherein said new encryption key is generated by said generator and transmitted by said wired network communications device at user-defined intervals.

11. (original) A wireless network as in claim 8, wherein when a newly generated encryption key is the same as one of k previously used encryption keys, said encryption key generator generates a new encryption key.

12. (original) A wireless network as in claim 11, wherein k is a user-defined number.

13. (cancelled)

14. (currently amended) A wireless network as in claim 8, further comprising a card tray at said updating device, said wireless network communications device being connected to said wired network by insertion of said wireless network communications device into said card tray.

15. (currently amended) A wireless network [[wireless]] station comprising:

a wireless network communications device for conducting wireless communications with a wired network, said wireless network communications device being physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable to a wired network to receive and store a new encryption key.

16. (previously presented) A wireless station as in claim 15, wherein said wireless network communications device is adapted to be physically connected to a wired network by being insertable into a card tray physically connected to said wired network.

17. (currently amended) A wireless network communications device comprising:

a removable wireless communications network card adapted to be physically connected to and disconnected from a wireless station card interface; a storage area on said network card which stores an updateable encryption key for use [[in]] by said wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface which supplies a new encryption key.

18. (previously presented) A wireless network communications card as in claim 17, wherein said card interface for providing a new encryption key is a PCMCIA card interface.

19. (previously presented) A wireless network communications card as in claim 18, wherein said PCMCIA card interface is provided at a PCMCIA card tray.

20. (currently amended) An encryption key programming system comprising:
an encryption key generator connected to a wired network; and
a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device, said wireless network communications device being accessible by a wireless network device for encrypted communications.

21. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a random encryption key.

22. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key at user-defined intervals.

23. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key on user-specified days.

24. (Previously Presented) An encryption key programming system as in claim 20, wherein said encryption key generator generates a first new encryption key, compares said new encryption key to the previous k encryption keys used in said network and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

25. (Original) An encryption key programming system as in claim 20, wherein k is a user-defined number of previously used encryption keys.

26. (Original) An encryption key programming system as in claim 20, further comprising a card tray connected to said programming device, said wireless communications device being received by said programming device by insertion of said wireless communications device into said card tray